

電子政府情報セキュリティ基盤技術開発事業
長期保存文書のための電子署名期限延長技術開発

電子文書長期保存技術検討コンソーシアム
宮崎一哉，篠原秀直，西岡秀司（三菱電機株式会社）
高山聡一郎（株式会社日立製作所）
木村道弘（日本電気株式会社）

概要

文書の電子化が進み、電子化文書の真正性を確保するためにデジタル署名が利用されつつある。ところが、デジタル署名には証明書の期限切れや失効などの制約があるため、電子文書を長期間保存しようとすると、長期経過後にデジタル署名の正当性を確認することができなくなってしまう。

そこで本技術開発では、電子化された文書の真正性を長期間維持するためのデジタル署名の有効性延長技術(電子署名延長技術)を開発することを目的とし、本技術に関わる方式検討をコンソーシアムにより実施し、署名延長サーバソフトウェアの基本機能及び署名延長クライアントソフトウェアを開発した。

今後、署名延長サーバソフトウェアの拡張機能開発及び検証実験を実施する予定である。

１．はじめに

政府は、2003 年度までに行政の効率化や国民負担の軽減を目標に行政手続きを電子化する電子政府の基盤を構築することを目指している。

電子政府の構築は、デジタル経済・社会の１つのモデルであり、その中で実施される情報セキュリティ確保のための対策もまた、広く民間の範となるものとなり、それによって、我が国のネットワーク全体の安全性・信頼性を高め、更に、具体的に進みつつある同様な取り組みと連携していくことにより国際的な貢献につながることも期待されている。このため、電子政府の構築に向けて、情報セキュリティ政策を重要なものとして位置づけ、積極的な貢献を行っていく必要がある。

本開発は、電子政府における情報セキュリティ確保のための基盤技術の開発を行うことを目的として、通商産業省の委託により実施するものの一つであり、平成 12 年 4 月に通商産業省が策定した「情報セキュリティ政策実行プログラム～電子政府のセキュアな基盤構築に向けての通商産業省の貢献～」の実施の重要な一部をなすものである。

電子政府では、電子化される申請や調達に関する書類の真正性を保証するために、公開鍵証明書に基づく電子署名が用いられるが、現在、公開鍵証明書には、数ヶ月乃至数年という有効期限が存在するほか、証明書記載事項変更／新規証明書使用開始／秘密鍵の危殆化などの理由による失効および電子署名に用いる暗号技術の脆弱化などによる公開鍵証明書の有効性について問題点等が指摘されている。例えば、受け付けた申請やそれに対する受領書を保存する場合、その真正性を公開鍵証明書の有効期限を越えて保証することができないことになり、その有効期間を超える期間を遡った過去の申請が偽造されていないことを保証することができないという事態が生じることになる。このように公開鍵暗号ベースの電子署名（デジタル署名）の有効性が、必然的に電子文書の真正性の保証にかかわることから、本開発により電子文書においても、紙が有している原本性の保証と同様に、長期にわたって真正性を確実に保証できる一手法を提言する。

２．研究開発の目標と内容

本技術開発の実施作業の構成は以下の通りである。

（１）方式設計

デジタル署名の有効性が連続性をともなって維持されていることを説明できる延長署名の書式、検証方式、デジタル署名の有効性延長機能を提供するサーバ（署名延長サーバ）とそのクライアント（署名延長クライアント）とのプロトコルの仕様をコンソーシアムによる検討を通して設計し、コンソーシアム標準案として仕様を公開する。

（２）機能開発

長期間有効性を維持すべきデジタル署名をクライアントソフトウェアより受け取り、予め判明している有効期限が切れる前に延長署名を生成し、データベースにて管理する署名延長サーバソフトウェアと、生成管理された延長署名を検証する機能を持つ署名延長クライアントソフトウェアを開発する。

（３）拡張機能開発

証明書記載事項変更、新規証明書使用開始、秘密鍵や証明書署名鍵の危殆化などの理由による失効や、デジタル署名に用いる暗号技術の脆弱化などに起因する、予知不可能な原因によるデジタル署名の有効性喪失に対処するための署名延長サーバの拡張機能開発する。

（４）検証実験

署名延長サーバ機能をインターネットを経由して利用できる第三者サービスとして提供しようとする際の妥当性を検証するための検証実験を実施する。

（５）セキュリティ評価対応作業

署名延長サーバソフトウェアに関して、評価保証レベル EAL2 のセキュリティ評価を受けるため、セキュリティターゲットの作成、脆弱性分析書の作成、訪問審査の受入等を行う。

また、上記（１）～（３）に関わる開発については、次の項目を満足することを目標とし、（４）の検証実験においては、次項を踏まえた本技術の妥当性を検証することを目標とする。

（１）　単にその時点で有効な最新の公開鍵証明書に基づく電子署名に付け替えるのではなく、最初に生成したオリジナルのデジタル署名の有効性が連続して維持されていることを客観的に示せること

（２）（１）を検証可能な完結したデータあるいはデータへのリンクとして管理し、第三者に提供できること

（３） デジタル署名の延長をオリジナルの署名者本人が行う必要はなく、第三者がサービスとして提供できること

（４）　ＰＫＩ（公開鍵基盤）に基づく標準的な技術（デジタル署名、タイムスタンプ、ＯＣＳＰなど）に立脚すること

（５）署名延長技術で生成された延長署名は本開発で提案する検証方式に準拠することにより、各社ＰＫＩ製品を利用して検証可能となること

なお、長期にわたって電子文書の真正性を保証する技術として、追記のみ可能で書換え不可能な特殊なハードウェアを用いる方法と署名者が係った過去の署名付き電子文書の圧縮情報を次々と綴り込む方法がある。前者の場合、真正性の検証にはそのハードウェアそのものを要すること、書換えが不可能であることを検証するには専門知識が必要であること、などの問題がある。また後者の場合、真正性検証のためには過去に行なったすべての電子署名が必要であり管理コストがかかること、他人が作成したデジタル署名を対象にすることが極めて困難である

こと、などの問題がある。
　本技術開発では、自己が作成したもの、他人が作成したものによらず、オリジナルの署名の有効性を第三者が容易に検証可能であるような完結したデータを生成／管理し、それを検証者の手元に容易に提供できる署名延長技術を開発することにより、電子文書の長期にわたる真正性を確保する上で生じる課題を克服することを目指す。

３．本年度の活動状況

　本年度の活動スケジュールは次の通りであった。

項目	平成１２年度						
	9月	10月	11月	12月	1月	2月	3月
方式設計	方式設計 ←→						
機能開発 サーバ機能		設計 ←→	開発 ←→		試験 ←→		
クライアント機能		設計 ←→	開発 ←→		試験 ←→		
拡張機能開発			機能設計 ←→				
検証実験						計画書作成 ←→	
セキュリティ評価		ST 作成 ←→			脆弱性分析書作成 ←→		訪問審査 ←→

以下、各作業項目について説明する。

3.1 方式設計

　前節に挙げた目標の（３）を満足するために、署名延長システムのアーキテクチャとしてはクライアント／サーバ方式を採用することとし、（４）を満足するために検証サービスやタイムスタンプサービスには標準的なＰＫＩサービスを利用することとした。

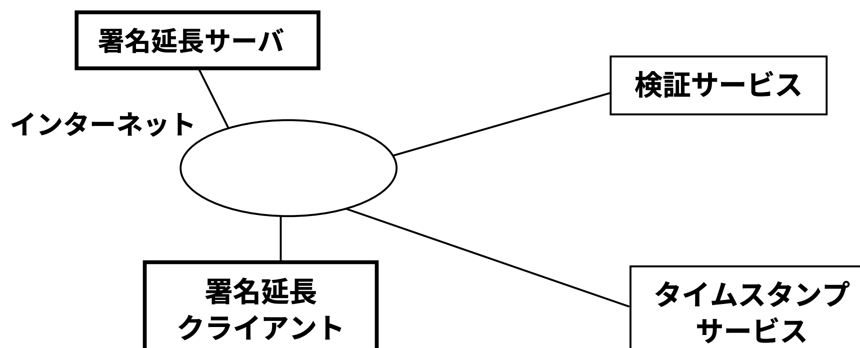


図１　署名延長システムの基本アーキテクチャ

このアーキテクチャを前提とし、更に目標（１）～（５）に配慮した上で、３社のコンソーシアムで実施した検討会により、次の基本仕様を決定した。

・延長署名フォーマット：

ETSI(the European Telecommunications Standards Institute)の Electronic Signature Formats をベースとして第三者によるサービスを可能とするように変更を加え、CMS(Cryptographic Message Syntax、RFC2630)の署名データ形式を拡張する形で延長署名のフォーマットを定義した。また、検証サーバには OCSP（Online Certificate Status Protocol）に基づくシステムを、タイムスタンプサーバには IETF において標準化策定中の Time Stamp Protocol に基づくシステムを利用することとした。

・延長署名の検証方式

上記延長署名フォーマットの検証アルゴリズムを決定するとともに、最初に生成したオリジナルのデジタル署名の有効性が連続して維持されていることを客観的に説明する検証レポートの形式を定義した。

・署名延長サーバと署名延長クライアント間のプロトコル

署名延長サービスをインターネット経由で提供できるようなリクエスト／レスポンスのプロトコルを定義した。

3.2 機能開発

署名延長システムの機能構成図を図２に示す。図中、ＶＡ（検証局）の機能およびＴＳＡ（タイムスタンプ局）の機能は既存のシステムを利用することとし、開発対象外とした。また、署名延長サーバ機能に含まれる延長署名自動生成機能は拡張機能として H13 年度に開発する予定である。H12 年度に開発した機能の概要は次の通りである。

（１）署名延長サーバ機能

署名延長クライアントからの署名延長要求を受け取り延長署名を生成／管理する機能、署名延長クライアントからの延長署名検証要求を受け取り延長署名を検証する機能、署名延長クライアントから延長署名系列要求を受け取り延長署名系列を署名延長クライアントに渡す機能、延長書名を生成管理する機能を提供する。

① 延長署名管理機能

署名延長クライアントとの通信および延長署名の管理を行う機能を提供する。

② 延長署名生成機能

署名延長クライアントから要求を受けた署名データに対して延長署名データを生成する機能を提供する。

③ 検証サーバ問合せ機能

延長署名を施す元となるデジタル署名（元署名）の有効性を保証するデータを得る機能を提供する。

④ タイムスタンプサーバ問合せ機能

生成した延長署名と延長署名を施す元となるデジタル署名（元署名）の有効性を保証するデータに対するタイムスタンプを得る機能を提供する。

⑤ 署名延長制御機能

デジタル署名が基づく公開鍵証明書が有効期限に到達する前に延長署名生成機能を呼び出す機能を提供する。

⑥ 延長署名検証機能

延長署名系列の検証を行い、その結果のレポートを生成する機能を提供する。

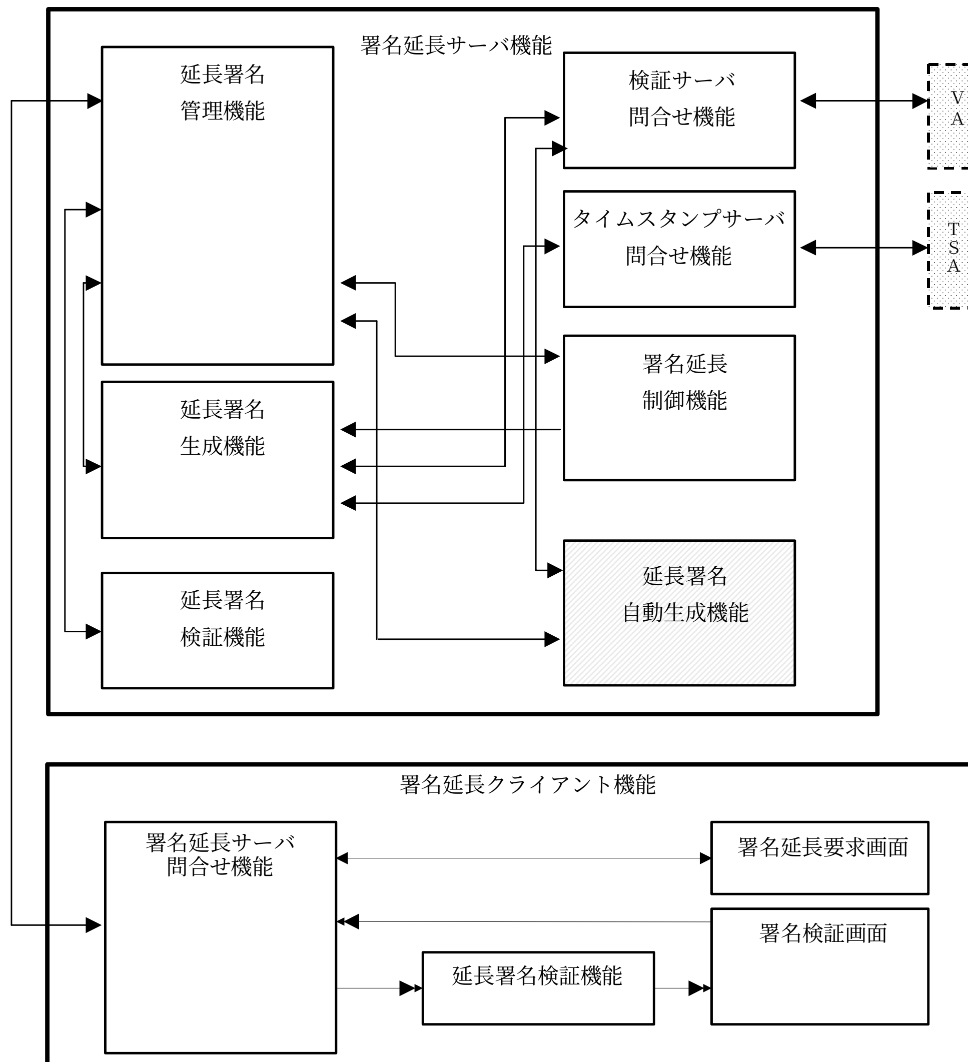


図２ 署名延長システム機能構成図

（２）署名延長クライアント機能

署名延長サーバ機能に対して各種要求／結果の送受信を行う機能と、署名延長サーバ機能から得た延長署名系列データを検証する機能を提供する。

① 延長署名検証機能
　延長署名系列データの検証を行い、その結果のレポートを生成する機能を提供する。

② 署名延長サーバ問合せ機能
　署名データの作成及び署名延長サーバ機能との通信を行う機能を提供する。

　署名延長サーバ機能を実現するソフトウェアの拡張機能以外の部分と署名延長クライアント機能を実現するソフトウェアをコンソーシアムメンバの２社がそれぞれ分担して開発した。
　署名延長システム開発は、ウォーターフォール型の開発工程を採用した。そのため、開発工程としては、機能設計、構造設計、コーディング、モジュール試験、結合試験、総合試験をこの順に行った。
　なお、機能設計を除いた工程は、拡張機能を除外した機能についてのみ実施した。

3.3 拡張機能開発

　署名延長サーバの拡張機能として、延長署名自動生成機能の開発を計画している。
　本機能は、デジタル署名の予期せぬ失効に対処し、デジタル署名が失効する前に延長署名を生成する機能を提供するものであり、以下の要件を満たす。
・タイムスタンプサーバの公開鍵証明書の失効に対処する
・署名延長に用いるタイムスタンプサーバの公開鍵証明書の有効期限、上記有効期限に対して何日前に延長署名を生成するか、仮延長署名生成の周期、署名延長に用いるタイムスタンプサーバ、およびその公開鍵証明書の有効性検証の周期をスケジュール管理データベースで管理する
・ スケジュールで決められた周期に基づいて延長署名を生成し、仮延長署名として延長署名系列毎に仮延長署名管理データベースで蓄積管理しておき、署名延長に用いるタイムスタンプサーバの公開鍵証明書の有効性が失われたとき、失効前に作成した仮延長署名を正規の延長署名として最新の延長署名として延長署名管理データベースの延長署名系列に加える。

　本拡張機能に関しては、H12 年度は機能設計のみを実施し、H13 年度に構造設計、コーディング、モジュール試験、結合試験、総合試験、をこの順に実施する予定である。

3.4 検証実験計画概要

　署名延長サーバ機能をインターネットを経由して利用できる第三者サービスとして提供しようとする際の妥当性を検証するために、H12 年度の機能開発及び H13 年度の拡張機能開発の成果物である署名延長システムをインターネットに接続し、署名延長クライアント機能から署名延長サーバ機能を利用する環境を想定した上で各種実験を実施することを計画している。
　検証項目として、次の項目を想定している。
・デジタル署名の問題点のカバー率の検証
・検証レポートの説得性の検証
・蓄積データ量の検証
・転送データ量の検証
・処理速度性能の検証
・相互運用性の検証

H12 年度は、その検証実験計画の概要を策定した。

3.5 セキュリティ評価対応作業

署名延長サーバソフトウェア（拡張機能を除く）に対して、評価保証レベル EAL2 のセキュリティ評価を受けるため、セキュリティターゲット、脆弱性分析書、その他セキュリティ評価対応ドキュメントの作成を実施した。また、セキュリティ評価チームによる訪問審査の受入を実施した。

４．外部発表及び成果物

4.1 外部発表

次の報告書内で、本テーマ実施内容を報告した。

・電子商取引推進協議会(ECOM) 認証･公証 WG 電子書名長期保存に関する中間報告(2001/03)

4.2 成果物

IPA に対する本年度の納入物件は次の通りである。

機能仕様書（拡張機能含む）	１部
構造仕様書（拡張機能除く）	１部
ソースプログラム（拡張機能除く）	１式
ロードモジュール（拡張機能除く）	１式
結合試験仕様書（拡張機能除く）	１部
結合試験報告書（拡張機能除く）	１部
総合試験仕様書（拡張機能除く）	１部
総合試験報告書（拡張機能除く）	１部
取扱説明書（拡張機能除く）	１部
セキュリティターゲット（拡張機能除く）	１部
脆弱性分析書（拡張機能除く）	１部
検証実験計画書	１部

５．今後の課題

今後の課題は次の通りである。
（１）　署名延長サーバの拡張機能として、延長署名自動生成機能の開発する。H12 年度開発では延長署名の有効期限にのみ対応していたが、拡張機能開発により、デジタル署名の予期せぬ失効に対処し、デジタル署名が失効する前に延長署名を生成する機能を提供する。
（２）署名延長サーバ機能をインターネットを経由して利用できる第三者サービスとして提供しようとする際の妥当性を検証するための実験を実施する。

６．まとめ

本技術開発において、デジタル署名によって電子文書の真正性を長期間保証するための署名延長技術における方式を設計し、その基本機能を開発した。署名延長サーバ機能開発にあたっては、評価保証レベル EAL2 のセキュリティ評価を受けた。更に、署名延長サーバの拡張機能の機能仕様を設計し、次年度実施予定の検証実験概要の策定を行った。

次年度は署名延長サーバの拡張機能を開発し、本署名延長技術が、電子文書の真正性の長期にわたる確保のためのサービスを提供できることを、検証実験を通して確認する予定である。

７．参考文献

・ETSI ES 201 733 Electronic Signature Formats
http://www.etsi.org/sec/ts_101733v010202p.pdf

・IETF Electronic Signature Formats for long term electronic signature
http://www.ietf.org/internet-drafts/draft-ietf-smime-esformats-03.txt

・IETF Time Stamp Protocol
http://www.ietf.org/internet-drafts/draft-ietf-pkix-time-stamp-13.txt

・IETF Cryptographic Message Syntax
http://www.csl.sony.co.jp/rfc/cache/rfc2630.txt.html

・Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP, RFC2560